Appl. No. 09/751,899
Amdt. Dated 04/03/06
Reply to Office Action of 12/06/2005
and Notice of Non-Compliant Amendment of 3/21/06

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method comprising:

authenticating a user of a platform during a Basic Input/Output System (BIOS) boot process;

releasing a first keying material from a token communicatively coupled to the platform in response to after authenticating the user during the BIOS boot process;

combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key during the BIOS boot process; and

using the combination key to decrypt a second BIOS area to recover a second segment of BIOS code during the BIOS boot process.

2. (Original) The method of claim 1 further comprising:

continuing the BIOS boot process.

3. (Previously Presented) The method of claim 1, wherein prior to authenticating the user, the method comprises:

loading a BIOS code including a first BIOS area and a second BIOS area, the first BIOS area being a first segment of the BIOS code encrypted with a keying material stored within an internal memory of a trusted platform module of the platform and the second BIOS area being a second segment of the BIOS code encrypted with the combination key.

4. (Original) The method of claim 3, wherein after loading of the BIOS code, the method further comprises:

decrypting the first BIOS area to recover the first segment of the BIOS code.

Appl. No. 09/751,899
Amdt. Dated 04/03/06
Reply to Office Action of 12/06/2005
And Notice of Non-Compliant Amendment of 3/21/06

5.   (Previously Presented) The method of claim 3, wherein the first segment of the BIOS is encrypted with the keying material and static information pertaining to the platform

6.   (Original) The method of claim 1 wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material.

7.   (Original) The method of claim 1, wherein authentication of the user is performed through biometrics.

8.   (Original) The method of claim 1, wherein the second keying material is stored within internal memory of a trusted platform module.

9.   (Original) The method of claim 1, wherein the second keying material is stored within a section of access-controlled system memory of the platform.

10.   (Original) The method of claim 1, wherein prior to authenticating the user, the method comprises:
        loading a BIOS code including a first BIOS area being a first segment of the BIOS code encrypted using a selected keying material; and
        loading an integrity metric including a hash value of an identification information of the platform.

11.   (Original) The method of claim 1, wherein the identification information includes a serial number of an integrated circuit device employed within the platform.

12.   (Cancelled).

13.   (Cancelled).

14.   (Cancelled).

Appl. No. 09/751,899
Amdt. Dated 04/03/06
Reply to Office Action of 12/06/2005
And Notice of Non-Compliant Amendment of 3/21/06

15. (Currently Amended) A platform comprising:

an input/output control hub (ICH);

a non-volatile memory unit coupled to the ICH, the non-volatile memory unit including a Basic Input/Output System (BIOS) code including a first BIOS area and a second BIOS area, the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code; and

a trusted platform module coupled to the ICH, the trusted platform module to produce a combination key during a BIOS boot process by combining a first incoming keying material released after authentication of a user of the platform with a second keying material internally stored within the platform and to decrypt the second BIOS area using the combination key to recover the second segment of BIOS code.

16. (Original) The platform of claim 15, wherein the trusted platform module to further decrypt the first BIOS area to recover the first segment of the BIOS code in an non-encrypted format.

17. (Original) The platform of claim 15 further comprising a hard disk drive coupled to the ICH.

18. (Original) The platform of claim 17, wherein the trusted platform module to further unbind keying material associated with the hard disk drive to access contents stored within the hard disk drive.

19. (Currently Amended) A program loaded into readable memory for execution by a trusted platform module of a platform, the program comprising:

code to decrypt a first Basic Input/Output System (BIOS) area during a BIOS boot process to recover a first segment of BIOS code;

code to produce a combination key during the BIOS boot process by combining a first incoming keying material released after authentication of a user of the platform with a second keying material internally stored within the trusted platform module; and

Appl. No. 09/751,899
Amdt. Dated 04/03/06
Reply to Office Action of 12/06/2005
And Notice of Non-Compliant Amendment of 3/21/06

code to decrypt a second BIOS area using the combination key to recover a second

segment of the BIOS code during the BIOS boot process.

20.   (Original) The program of claim 19, wherein the first BIOS area is the first

segment of the BIOS code encrypted with a keying material and the second BIOS area is the

second segment of the BIOS code encrypted with the combination key.

21.   (Original) The program of claim 19 further comprising:

code to unbind keying material associated with a non-volatile storage device for

accessing contents stored within the non-volatile storage device.

22.   (Previously Presented) The method of claim 5, wherein the static information is a

serial number or a hash value of the serial number associated with hardware within the platform.

23.   (Previously Presented) The integrated circuit device of claim 12 being

implemented within a platform and coupled to an input /output control hub in communication

with a processor of the platform.